UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

A gold iPhone with serial number FDFVVG32CX

Case No. 1:24MJ 379

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
See Attachment A.

located in the Middle District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§2251(a) and (e)	Conspiracy to Produce Child Pornography
18 U.S.C. §2252A(a)(2)(A)	Receipt and Distribution of Child Pornography
18 U.S.C. §2252A(a)(5)(B)	Possession of and/or Access with Intent to View Child Pornography

The application is based on these facts:
See attached affidavit incorporated by reference herein

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/S/ Lauren Darden
Applicant's signature

Lauren Darden/FBI Special Agent
Printed name and title

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date: 9/26/2024

Judge's signature

City and state: Winston-Salem, North Carolina

JOI ELIZABETH PEAKE, United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Special Agent Lauren Darden, with the Federal Bureau of Investigation (FBI), being duly sworn, deposes and states the following:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since March 2019. I am an investigative or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7). That is, I am an officer of the United States, who is empowered by law to conduct investigations of, and make arrests for, violations of federal law, including the offenses enumerated in 18 U.S.C. §§ 1591, 2251 and 2252, et seq.

2. I am currently assigned to the FBI's Child Exploitation and Human Trafficking Task Force, Raleigh Resident Agency out of the Charlotte Division, which targets individuals involved in the online sexual exploitation of children. As part of my duties, I investigate crimes involving the sexual exploitation of minors, including sex trafficking, child pornography, and enticement violations. I have received training on the proper investigative techniques for these violations, including the use of surveillance techniques, undercover activities, and the application and execution of arrest and search warrants. I have conducted and assisted in child exploitation investigations and human trafficking investigations. Prior to my current assignment, I was assigned to the FBI Miami Division, where I was assigned to the violent crimes against children and human trafficking squad.

3. This affidavit is submitted in support of a search warrant pursuant to Rule 41of the Federal Rules of Criminal Procedure for a warrant to search:

- (1) Gold Apple iPhone cellular telephone with serial number FDFVVG32CX (hereinafter, the "gold Apple iPhone" or "**Subject**

Device"), as further described in Attachment A, which is currently in the custody of the Durham Police Department located at 602 E Main Street, Durham, North Carolina 27701. This includes Telegram data associated with username "@Malachaiotto" with a display name of "Mav Z" and linked to phone number 305-610-1913 (hereinafter, the "Mav Z Account"). Specifically, affiant believes that this Telegram account is linked to the Subject Device and that powering on the Subject Device and enabling its internet connection will allow law enforcement to review, copy and download information from the Mav Z Account.

4. Based on the facts set forth in this affidavit, I submit that there is probable cause to believe that violations of 18 U.S.C. §§ 2251(a) and (e), 2252A(a)(2)(A) and 2252A(a)(5)(B), that is, conspiracy to produce child pornography, and the receipt, distribution, possession, and access with intent to view child pornography (collectively, the "Subject Offenses") have occurred and that evidence and instrumentalities of the Subject Offenses as described in Attachment B will be found on the Subject Device as described in Attachment A.

5. Accordingly, this affidavit is made in support of an application for a warrant authorizing a search of the Subject Device for evidence and instrumentalities of the Subject Offenses, as described in Attachment B. Attachments A and B are incorporated herein by reference.

6. The Court has jurisdiction to issue the proposed warrants under Rule 41(b)(1), as the property to be searched and seized is located within the Middle District of North Carolina. [1]

[1] Your affiant believes that pursuant to Rule 41(b)(6)(A), the Court can also issue a warrant for remote access to seize and copy electronically stored information of Telegram accessed through the phone for which the location of the information is concealed through technological means.

7. The information set forth in this affidavit is based upon my personal knowledge of this investigation and information conveyed to me by others involved with the investigation, including others with knowledge regarding both the technical aspects of Telegram and how it stores its data. Since this affidavit is being submitted for the limited purpose of establishing probable cause for the requested search warrant, I have not included every detail of every aspect of the investigation known to me or to the government. Rather, the following paragraphs set forth only those facts necessary to support a finding of probable cause.

STATUTORY AUTHORITY

8. 18 U.S.C. §§ 2251(a) and (e) prohibits the production of visual depictions of a minor engaged in sexually explicit conduct. Conspiracies and attempts are also violations of this statute.

9. 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) prohibits a person from knowingly receiving or distributing child pornography, as defined in 18 U.S.C. § 2256(8), using any means and facility of interstate and foreign commerce, that has been mailed, or that has been shipped and transported in and affecting interstate and foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute.

10. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute.

DEFINITIONS

11. The following definitions apply to this Affidavit and its Attachments:

a. 18 U.S.C. § 2256(1) defines "minor" as any person under the age of eighteen years.

b. 18 U.S.C. § 2256(8) defines "child pornography" in relevant part as "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where … the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. Child sex abuse material or "CSAM" has the same meaning.

c. 18 U.S.C. § 2256(2) defines "sexually explicit conduct" as actual or simulated: (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the anus, genitals, or pubic area of any person.

d. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or by electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

e. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

f. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

g. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other highspeed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

h. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

i. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN OR VISUAL DEPICTIONS OF CHILDREN

12. Based upon my training and experience, as well as upon information provided to me by other law enforcement officers, there are certain characteristics common to individuals who

receive, possess and/or access with intent to view child pornography, which may be exhibited in varying combinations:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses (such as in person, in photographs, or other visual media), or from literature describing such activity. Due to the accessibility and availability of child pornography on the Internet, in my recent experience, instead of maintaining collections, some offenders engage in a pattern of viewing or downloading child pornography online and then deleting the material.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. They may also use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections can be maintained for several years to enable the individual to view the collection, which is valued highly.

d. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

e. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

f. Individuals whose sexual interest in children or images of children has led them to purchase access to paid websites or other commercial sources of child pornography frequently maintain the financial records of those transactions at their residences.

BACKGROUND CONCERNING TELEGRAM

13. Telegram Messenger (also known as "Telegram") is a cloud-based mobile and desktop messaging application purportedly owned and/or controlled by Telegram Messenger Inc. Telegram can be used on smartphones, such as Apple iOS and Google Android devices, and on desktop computers, by users to send messages and media to each other.

14. To sign up for a Telegram account, a user must provide a phone number. Telegram users can also select a username but are not required to. Usernames are unique, meaning only one user can have a particular username. Users can also select a display name, such as a first and last name. Display names are not unique.

15. Telegram is supported on various devices including smartphones, tablets, desktop computers and laptop computers, and Telegram can by synced on multiple devices at the same time. A user can log into Telegram using a phone number from as many devices as that user likes, even simultaneously. Unless a user enables a "lock" on the Telegram application, which may include two-factor authentication, anyone who gains access to an unlocked smartphone, tablet, or computer running Telegram will be able to access and view a user's Telegram account.

16. Telegram offers a variety of communication methods for its users:

a. **Chats**. Users on Telegram can communicate with each other through chats. They can send each other text messages, photos, videos, any files, and make voice calls.

b. **Secret Chats**. Secret chats use end-to-end encryption, which means only the sender and recipient have the ability to view the content of the chats. These secret chats also disappear and can be set to self-destruct.

c. **Groups.** Telegram allows collections of users to communicate with each other in chat rooms called groups. Groups may be by invitation only.

17. According to Telegram's privacy policies, Telegram stores basic user account data, including mobile number, profile name, profile picture, screen names, and e-mail address, to the extent a user has provided this information.[2] Telegram also stores messages, photos, videos and documents from a user's chats and private messages, as well as from public channels and public groups in which the user participates. As discussed below, most content is distributed and stored in various unknown locations. In addition, content generally is encrypted and stored in a way that prevents Telegram from being able to access the content in unencrypted form.

[2] https://telegram.org/privacy (last visited September 3, 2024).

18. Telegram was founded in Russia, but, according to its website, it purportedly "has tried a number of locations as its base," and currently its "development team is based in Dubai."[3]

19. The locations of Telegram's data centers are not publicly disclosed. In addition, Telegram uses various technological means to conceal the location of electronically stored information. As stated on the Telegram website:

> To protect the data that is not covered by end-to-end encryption, Telegram uses a distributed infrastructure. Cloud chat data is stored in multiple data centers around the globe that are controlled by different legal entities spread across different jurisdictions. The relevant decryption keys are split into parts and are never kept in the same place as the data they protect. As a result, several court orders from different jurisdictions are required to force us to give up any data.
>
> Thanks to this structure, we can ensure that no single government or block of like-minded countries can intrude on people's privacy and freedom of expression. Telegram can be forced to give up data only if an issue is grave and universal enough to pass the scrutiny of several different legal systems around the world.
>
> To this day, we have disclosed 0 bytes of user data to third parties, including governments.[4]

Telegram's description of a "distributed infrastructure" is somewhat at odds with other information Telegram has provided. Currently, Telegram states that UK or the Economic European Area account data "is stored in data centers in the Netherlands."

20. Telegram's website does not state where United States account data is stored. In a 2014 tweet, Telegram stated it used "San Francisco" servers "for American" data. Publicly available information obtained from the Telegram application programming interface (API) has identified U.S.-based IP addresses as access points to Telegram data centers, indicating that either

[3] https://telegram.org/faq (last visited September 3, 2024).

[4] https://telegram.org/faq#q-do-you-process-data-requests (last accessed September 5, 2024).

a proxy service or an actual data center is located in the United States. For that reason, law enforcement has reason to believe that Telegram maintains at least some server infrastructure in the U.S. As a result, any search of the Telegram servers would not be a wholly extraterritorial search.

21. Even if law enforcement knew where United States account data is stored, , Telegram states that the information stored at its data centers is "heavily encrypted so that local Telegram engineers or physical intruders cannot get access" and notes that "encryption keys . . . are stored in several other data centers in different jurisdictions."[5] As the Telegram website explains with respect to Secret chats:[6]

> *Secret chats* use end-to-end encryption. This means that all data is encrypted with a key that only you and the recipient know. There is **no way** for us or anybody else without direct access to your device to learn what content is being sent in those messages. We do not store your secret chats on our servers. We also do not keep any logs for messages in secret chats, so after a short period of time we no longer know who or when you messaged via secret chats. For the same reasons secret chats are not available in the cloud — **you can only access those messages from the device they were sent *to* or *from*.**
>
> **3.3.3. Media in Secret Chats**
> When you send photos, videos or files via secret chats, before being uploaded, each item is encrypted with a separate key, not known to the server. This key and the file's location are then encrypted again, this time with the secret chat's key — and sent to your recipient. They can then download and decipher the file. This means that the file is technically on one of Telegram's servers, but it looks like a piece of random indecipherable garbage to everyone except for you and the recipient. We don't know what this random data stands for and we have no idea which particular chat it belongs to. We periodically purge this random data from our servers to save disk space.

[5] https://telegram.org/privacy (last visited on September 16, 2024)
[6] *Id.* (emphasis added)

22. Telegram advertises that it provides server-client encryption for private and group chats, and optional client-client encryption for chats and video calling.[7] Some Telegram users likely use its services to address legitimate concerns to keep online information private. However, in my training and experience, Telegram is known to law enforcement as a tool used by some individuals for the purpose of discussing or even furthering criminal activity because those individuals believe that their communications are untraceable due to the application's encryption option. Multiple newspaper articles have even described Telegram as the "app of choice" for terrorists.[8] In my training and experience with investigating child exploitation cases and from speaking with other law enforcement agents, I am aware that some individuals who traffic in child sexual abuse material use Telegram because they believe their communications are untraceable due to Telegram's encryption option.

23. Ultimately, in my training and experience, Telegram's business model is designed to conceal information related to customer accounts in the United States and elsewhere through technological means.

---

[7] https://telegram.org/faq#q-so-how-do-you-encrypt-data (last visited on September 16, 2024).

[8] *See, e.g.*, Ben Quinn, *Telegram is warned app 'nurtures subculture deifying terrorists'* (Oct. 14, 2021), https://www.theguardian.com/uk-news/2021/oct/14/telegram-warned-of-nurturing-subculture-deifying-terrorists ("The risk of radicalisation has grown on some platforms after sweeping bans on larger, more mainstream platforms encouraged many conspiratorial networks to migrate to often largely unmoderated alternatives such as Telegram, the report says."); Maggie Rowland, *Extremism and Encryption: Terrorists on Telegram* (Aug. 10, 2017), https://www.hsdl.org/c/extremism-and-encryption-terrorists-on-telegram/ ("Telegram is now the app of choice for terrorist propaganda, communication, and organization."); Jessica Clarence, *The trouble with Telegram (part 1)* (Jul. 11, 2018), https://www.aspistrategist.org.au/the-trouble-with-telegram-part-1/ ("Telegram is also structured to resist government requests and subpoenas. It's incorporated in Dubai, but its servers' locations and employees' names are secret, thanks to a complex of transnational shell companies scattered worldwide. Access to user data requires not only international cooperation, but knowing where the data is located—a nearly impossible task without cooperation from the messaging service.").

JURISDICTION

24. This Court has jurisdiction to issue the requested warrant under Rule 41(b)(1), as the property to be searched and seized is located within the Middle District of North Carolina.[9] In addition, the below facts establish that there is probable cause to believe that activities related to the Subject Offenses being investigated occurred within this judicial district. As discussed more fully below, acts or omissions in furtherance of the Subject Offenses under investigation occurred within the Middle District of North Carolina. *See* 18 U.S.C. § 3237.

PROBABLE CAUSE

25. On April 21, 2024, New York State Police (NYSP) Troop K received a Cyber Tip report number 192060652, which was submitted by X Corp (formerly known as Twitter) regarding an account which contained apparent child pornography. The report indicated the images appeared to be newly produced and/or homemade content. NYSP identified the user of the account in question as an individual with a specified residential address New York. A search warrant was executed at the residence in New York and items of evidence were seized. The investigation revealed the individual was producing child pornography with her 8-month-old daughter in a town in New York, known to your affiant. She also distributed the Child Pornography to unknown individuals. On April 21, 2024, the individual in New York was arrested, and a forensic extraction of her device was conducted. During a review of the forensic extraction, a chat group was located which consisted of users who asked the individual to produce child pornography for them. A user with the X account ID 1776874530016800768 and username "Makinitwett" ("Makinitwett Account") was observed in this chat group.

---

[9] Your affiant believes that pursuant to Rule 41(b)(6)(A), the Court can also issue a warrant for remote access to seize and copy electronically stored information of Telegram accessed through the phone for which the location of the information is concealed through technological means.

26. On May 2, 2024, a subpoena was submitted to X Corp10 to identify the subscriber of Makinitwett Account. On May 7, 2024, X provided return information associated with the X account which indicated the creation IP address was "107.15.232.208" and the email address sociated with the account was "boxx1842@gmail.com." On or about May 9, 2024, a subpoena was sent to Charter Communications, Inc. for the user identification for the IP address "107.15.232.208." The subscriber was identified as Laquasha Roache with a service address of 3004 Ivey Wood Lane, Apartment 114, Durham, North Carolina 27703.

27. X messages between the individual in New York and Makinitwett Account were located for the time period of April 20, 2024, through April 21, 2024. The individual in New York told Makinitwett Account she had an 8-month-old daughter and the thought of her being used turned her on. Makinitwett Account talked about the baby's vagina in a vulgar manner and indicated he had sex with minors. Makinitwett Account indicated he engaged in sexual acts with his sister beginning at 6 months old even stating, "I was putting tip in her at 1." A portion of the statements made by Makinitwett Account in chats with the individual in New York on April 21, 2024, are as follows:

- "Show me her holes while she sleep"
- "I use to fuck my lil sister and eat her cunnie"
- "Most of my bodies under 16"
- "Rub her clit for me"
- Eat her, lick her, spread her cunnie more"

[10] X Corp. owns and operates X (previously known as Twitter), a social networking and microblogging service that can be accessed at http://www.x.com, http://www.twitter.com, and via the X mobile application ("app"). Generally, after creating an X account, users can personalize their account profile page and view, send, and receive communications via the platform.

- "Can you send more spreading it Nd rubbing rn?"

28. The individual in New York asked Makinitwett Account if they could chat on another platform because she did not think they were supposed to be sending those type of pictures on X. Makinitwett Account suggested Telegram. The individual in New York provided her Telegram to Makinitwett Account, told him to delete the conversation on Twitter, and said she would send pictures on Telegram. The account used by the individual in New York on Telegram is known to law enforcement. Telegram chats between the individual in New York and username "@Malachaiotto" and display name "Mav Z" (Mav Z Account) were also located. On April 21, 2024, at 04:46:29 AM UTC, the Mav Z Account sent the individual in New York a message on Telegram which said "hey." On or about April 21, 2024, at 04:46:41 UTC, Makinitwett Account sent the individual in New York a message on X that said, "Got my text?" On April 21, 2024, at 04:47:01 UTC, Mav Z Account told the individual in New York, "I deleted it" and "Send them here," in which she responds with sending five images of a baby's exposed vagina on Telegram. The timestamps and conversations in the Telegram chats appeared to match up with the Twitter conversations indicating the user of Makinitwett Account used Mav Z Account on Telegram. The New York Individual asked Mav Z Account if he was attracted to any other babies to which he replied, "Any with they pussy out," "I work retail a lot of kids who come in look fuckable," "Like any real cute babies id fuck idc," "I love baby cunt." Mav Z Account also distributed videos depicting child pornography to the individual in New York on April 21, 2024, at 04:59:24 AM UTC. The files distributed to the individual by Mav Z Account were reviewed. Two of those files are described below:

- File name: telegram-cloud-document-5-6127152648861781744 is a video file which depicts an adult male rubbing his erect penis on a baby's mouth

and inserting the tip of his penis in the baby's mouth.

- File name: telegram-cloud-documents-5-6127152648861781746 is a videos file which depicts a pre-pubescent female performing oral sex on an adult male.

29. An emergency disclosure request was submitted to Google, Inc. for subscriber information and any recovery telephone numbers, email accounts, and IP addresses associated with boxx1842@gmail.com. Google provided subscriber information for the account which indicated the account had the recovery telephone number 305-610-1913. Telephone subscriber information was requested and indicated an account holder name of La'Quan Rigby (TARGET SUBJECT). Database and baseline checks were conducted, and the TARGET SUBJECT provided the telephone number 305-610-1913 and a residential address of 3004 Ivey Wood Lane Apartment 114, Durham, North Carolina 27703, to law enforcement as a witness of a theft at the Family Dollar where he was employed.

30. North Carolina state arrest warrants were obtained for the TARGET SUBJECT for Second Degree Sexual Exploitation of a Minor. On June 28, 2024, surveillance was conducted at 3004 Ivey Wood Lane, Apartment 114, Durham, North Carolina. The TARGET SUBJECT was observed leaving the apartment. Law Enforcement contacted the TARGET SUBJECT at 414 E. Main Street, Durham, North Carolina 27701 and he was arrested. At the time of his arrest, he was in possession of the gold Apple iPhone enclosed within a clear case with a dragon sticker on the back of the case.

31. Law enforcement advised the TARGET SUBJECT of his rights. He waived rights, signed the waiver, and agreed to speak to investigators. The TARGET SUBJECT admitted to corresponding online with other users on X and Telegram regarding child pornography. He also

admitted to receiving child pornography from other users. He confirmed most of the activity was conducted on his gold Apple iPhone, which was seized from his person at the time of the arrest. A state search warrant was obtained for the TARGET SUBJECT's cellular phone and a forensic image of the telephone ("forensic extraction") was subsequently completed.

32. A review of the forensic extraction revealed that Telegram was downloaded on Rigby's gold Apple iPhone on September 16, 2020. Additionally, the Mav Z Account was located on the device. There were also conversations between Mav Z Account and unknown individuals located within the forensic extraction. Mav Z Account had conversations with a Telegram account with the display name "Saya" in or around May 2024. A review of this conversation indicated Mav Z Account distributed videos to "Saya." Mav Z Account asks "Saya" if they wanted to see "toddlers and real young babies" and if they wanted "to hear them cry as they get raped hard by dad." After a brief exchange, Mav Z Account sent approximately fifteen videos. The content of the videos is not visible in the phone extraction, but based on the conversation following the videos, it indicates the videos contained child pornography. After sending the videos, Mav Z Account called "Saya" a "pedo pup" and said, "Don't lie and act like you didn't get wet watching those kid holes get used." There was another Telegram chat located between Mav Z Account and an unknown user with a user ID of 6854932921. In these chats, they share videos back and forth. The videos are not visible in the phone extraction, but based on the conversations surrounding the videos, it appears the videos contain child pornography. Mav Z Account indicates wanting his daughter like that while she is watching kid shows in response to a video he received. Mav Z Account also communicated with a Telegram user with the name "CP Share." In these conversations, Mav Z Account and "CP Share" are discussing trading. Based on the name of the group, it is believed Mav Z Account traded child pornography with the "CP Share" account.

33. During the manual review of the Subject Device as it was in airplane mode, law enforcement located multiple social media applications on the Subject Device including the application Telegram. Law enforcement opened the Telegram application and several conversations appeared. Chats and the thumbnails of images were visible when law enforcement opened the application. However, when law enforcement attempted to click on the individual chats, some of the information or files would not load. Multiple messages and files can be seen as being exchanged between the users. However, some of the files exchanged are blurred out. I know based on my training and experience and from speaking with other law enforcement officers and forensic examiners that files appearing blurred on the phone or conversations/data not loading is indicative the files are not stored locally in the device, rather they are stored on Telegram's servers.

34. Based on the manual review of the cellular phone in airplane mode, I know there were files of child pornography distributed and received that were not retrieved during the forensic extraction of the Subject Device on airplane mode.

35. Your affiant believes that by powering on the Subject Device and enabling the internet connection, information from the Telegram Account will download to the device and this would be useful in order to obtain complete communications and files exchanged between users regarding the conspiracy to produce child pornography and the receipt, distribution, possession, and access with intent to view child pornography.

THE SEARCH OF THE DEVICE

36. I request authority to search Subject Device to include powering on the Subject Device, enabling its internet connection, allowing information, including that from Telegram, to download to the device and review, copy and download information, including that from the Telegram application on the phone.

37. If law enforcement accesses the Mav Z Account by powering on the Subject Phone and enabling its internet connection, the forensic expert will conduct a limited search of that Subject Device, which will include a search of the Telegram application and then re-imaging the phone or copying the contents of the Telegram Account containing the Mav Z Account Information.

38. Once the Mav Z Account Information has been seized or copied onto electronic media in this district, law enforcement will power down the Subject Device.

39. The search technique is designed to collect the items described above and in Attachment B, i.e., Telegram chats, secret chats and group communications which may be evidence of violations of the Subject Offenses described above.

40. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would authorize the copying of electronically stored information from the Subject Device as described in Attachment A and the later review of that information consistent with the warrant in order to identify electronically stored information particularly described in Attachment B.

CONCLUSION

41. Based on the foregoing, I have probable cause to believe that violations of federal criminal laws 18 U.S.C. §§ 2251(a) and (e), 2252A(a)(2)(A) and 2252A(a)(5)(B), that is, conspiracy to produce child pornography and the receipt, distribution, possession, and access with intent to view child pornography, have been committed, and that evidence of those crimes, as more fully described in Attachment B, will be found on the Subject Device, including the Mav Z Account which is associated with the Subject Device, as described in Attachment A.

42. Because the search does not involve the physical seizure of tangible property not

already in law enforcement possession and the execution of this warrant does not involve the physical intrusion onto a premises, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

/s/ Lauren Darden
Lauren Darden
Special Agent, Federal Bureau of Investigation

Pursuant to Rule 4.1 of the Federal Rules of Criminal Procedure, the affiant appeared before me via reliable electronic means (telephone), was placed under oath, and attested to the contents of this written affidavit.

HON. JOI ELIZABETH PEAKE
UNITED STATES MAGISTRATE JUDGE
MIDDLE DISTRICT OF NORTH CAROLINA

ATTACHMENT A

Property to be searched

(1) Gold Apple iPhone cellular telephone, with serial number FDFVVG32CX (hereinafter, the "Subject Device"), currently in the custody of the Durham Police Department located at 602 E Main Street, Durham, North Carolina 27701. This includes Telegram data associated with username "@Malachaiotto" with a display name of "Mav Z" and linked to phone number 305-610-1913 (hereafter, the "Mav Z Account") that is linked to the device. The government is authorized to power on the Subject Device and enable its internet connection to allow law enforcement to review, copy and download information from the Mav Z Account.

ATTACHMENT B

Items to be seized

For the time frame of 09/16/2020 (when Telegram was downloaded on the Subject Device) through 06/28/2024, any and all evidence and instrumentalities of violations of 18 U.S.C. §§ 2251(a) and (e), 2252A(a)(2)(A) and 2252A(a)(5)(B), that is, the conspiracy to produce child pornography and the receipt, distribution, possession, and access with intent to view child pornography, in the form of the following:

1. Records identifying the users of the Mav Z Account;

2. Records of names, phone contacts, phone numbers, phone call lists, incoming calls, outgoing calls, missed calls;

3. Messages, including chat messages, secret chats messages, and group messages or recorded voice messages, which may reflect communications with co-conspirators and/or victims;

4. GPS location information, maps, saved points, and any other information identifying or describing the location of the user of the device described in Attachment A.

5. Evidence of who used, owned, or controlled the Mav Z Account at the time the things described in this warrant were created, edited or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, user profiles, messages and message logs, photographs, and correspondence;

6. Evidence of the time the Mav Z Account described in Attachment A was used;

7. Contextual information necessary to understand the evidence described in this attachment.

8. Child pornography.

9. Child erotica.

10. All images depicting any individual who is depicted in child pornography or child erotica.

11. Records and information referencing or revealing the trafficking, advertising, or possession of child pornography, to include the intent of the individuals involved and the location of the occurrence.

12. Records and information revealing the sexual exploitation of or sexual interest in any minor, to include the identity of the individuals involved and the location of occurrence.